# United States District Court

FOR THE
**NORTHERN DISTRICT OF CALIFORNIA**

VENUE: SAN FRANCISCO



UNITED STATES OF AMERICA,

V.

ALEXEI VIKTOROVICH BILUCHENKO,
a/k/a "Alexsey Viktorovich Bilyuchenko,"
a/k/a "Алексей Викторович Билюченко"

DEFENDANT(S).

# INDICTMENT

18 U.S.C. §§ 1960, 2 – Operation of an Unlicensed Money Services Business
18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering

A true bill.

/s/ Foreperson of the Grand Jury
Foreman

Filed in open court this 12th day of

July 2022.

Stephen Ybarra
Clerk

Bail, $ Warrant

Hon. Alex G. Tse, United States Magistrate Judge

STEPHANIE M. HINDS (CABN 154284)
United States Attorney



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| UNITED STATES OF AMERICA,<br><br>Plaintiff,<br><br>v.<br><br>ALEXEI VIKTOROVICH BILUCHENKO,<br>a/k/a "Alexsey Viktorovich Bilyuchenko,"<br>a/k/a "Алексей Викторович Билюченко"<br><br>Defendant. | CASE NO. 3:22-cr-00255 VC<br><br>VIOLATIONS: 18 U.S.C. §§ 1960, 2 – Operation of an Unlicensed Money Services Business; 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering; 18 U.S.C. § 982(a)(1) – Criminal Forfeiture<br><br>SAN FRANCISCO VENUE |

# INDICTMENT

The Grand Jury charges:

## Introductory Allegations

At all times relevant to this Indictment:

1. Defendant ALEXEI VIKTOROVICH BILUCHENKO was a Russian citizen residing in Russia.

2. From in or around 2011 to in or around July 2017, BTC-e was a digital currency exchange controlled by Alexander Vinnik, ALEXEI VIKTOROVICH BILUCHENKO, and others.

3. [redacted]

[redacted]

BTC-E BACKGROUND

4. From its inception in or around 2011 until it was shut down by law enforcement in or around July 2017, BTC-e was one of the world's largest digital currency exchanges. In the years it operated, BTC-e processed several billion dollars' worth of transactions and served over one million users worldwide, including numerous customers in the United States and customers in the Northern District of California.

5. BTC-e was one of the primary ways by which cyber criminals around the world transferred, laundered, and stored the criminal proceeds of their illegal activities. BTC-e received criminal proceeds of numerous computer intrusions and hacking incidents, ransomware events, identity theft schemes, corrupt public officials, and narcotics distribution rings.

6. Because such a significant portion of BTC-e's business was derived from criminal activity, and given its global reach, the scope of the unlawful conduct was massive. During the relevant timeframe from in or around 2011 to in or around 2017, BTC-e processed millions of bitcoin worth of deposits and withdrawals.

7. Users could create BTC-e accounts with only a username, password, and email address. A BTC-e user did not need to provide even the most basic identifying information such as name, date of birth, address, or other identifiers. Unlike legitimate payment processors or digital currency exchanges, BTC-e did not require its users to validate their identity information by providing official identification documents.

8. Thus, a user could create a BTC-e account with nothing more than a username and email address, which often bore no relationship to the identity of the actual user. Accounts were therefore easily opened anonymously, including by customers in the United States within the Northern District of California.

9. Once a user created an account, they could use it to send and receive bitcoin, or one of several other digital currencies that BTC-e supported. BTC-e held funds on behalf of their customers in digital currency wallets secured on BTC-e's servers. BTC-e allowed users to purchase digital currency and fund their accounts through BTC-e's affiliated financial "partners." BTC-e also allowed users to transfer funds from one BTC-e account to another through "BTC-e code" or "vouchers," which

functioned like a transferable gift card. BTC-e's business model obscured and anonymized transactions and source of funds.

10. Despite doing substantial business in the United States, BTC-e was not registered as a money services business with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), as federal law requires. BTC-e had no anti-money laundering and/or "Know-Your-Customer" (KYC) processes and policies in place, as federal law also requires. Indeed, BTC-e collected virtually no customer data at all. As such, it was attractive to those who desired to conceal criminal proceeds, as it made it more difficult for law enforcement to trace and attribute funds.

11. BTC-e relied on shell companies and affiliate entities that were similarly unregistered with FinCEN and lacked basic anti-money laundering and KYC policies. These entities catered to an online and worldwide customer base, and electronically "muled" fiat currency in and out of BTC-e.

12. BTC-e maintained its servers in the United States. The servers were one of the primary ways in which BTC-e and its operators effectuated their scheme. BTC-e used third-party companies, including companies within the Northern District of California, to effectuate its operations.

BTC-E'S CRIMINAL DESIGN

13. As described above, BTC-e's system was designed so that criminals could accomplish financial transactions with anonymity and thereby avoid apprehension by law enforcement or seizure of funds.

14. BTC-e was thus used extensively for illegal purposes and functioned as the exchange of choice to convert digital currency like bitcoin to fiat currency for the criminal world.

15. The BTC-e operators were aware that BTC-e functioned as a money laundering enterprise. Messages on BTC-e's public message board openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged, and how they used BTC-e to launder funds.

16. BTC-e users established accounts under monikers suggestive of criminality, including monikers such as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire."

17. Criminals used BTC-e to launder criminal proceeds and transfer funds among criminal

associates. In particular, BTC-e was used by hacking and computer intrusion rings operating around the world to distribute criminal proceeds of their endeavors. It was also used by rings of identity thieves, corrupt public officials, narcotics distribution networks, and other criminals.

18. Some of the earliest significant purveyors of ransomware used BTC-e as a means of storing, distributing, and laundering their criminal proceeds. Ransomware is a practice in which cyber criminals orchestrate the unwanted malicious download of encryption software on an unsuspecting victim computer. It works as follows: once a victim is infected with the malicious software, often by clicking on a malicious link or opening an infected email, the ransomware will encrypt multiple file types on victim machines and hold those files for ransom, requiring the victim to pay the perpetrators of the ransomware scheme in order to have their files decrypted. The only payment methods accepted by purveyors of modern ransomware are bitcoin and other forms of digital currency.

19. One such ransomware scheme, CryptoWall, was distributed by methods including phishing emails. CryptoWall was one of the most infamous varieties of ransomware and infected countless computers across the world. During the timeframe relevant to this Indictment, the purveyors of CryptoWall deposited and laundered many hundreds of thousands of dollars' worth of ransom payments into BTC-e.

20. BTC-e also served as the receptacle and transmitter of criminal funds from a series of well-publicized computer intrusions and resulting thefts.

[redacted]

[redacted]

STATUTORY ALLEGATIONS

COUNT ONE: (18 U.S.C. § 1960 – Operation of an Unlicensed Money Transmitting Business)

27. The factual allegations in paragraphs 1 through 26 are re-alleged and incorporated herein as if set forth in full.

28. From in or around 2011, continuing through a date unknown to the grand jury but no later than in or around 2018, both dates being approximate and inclusive, in the Northern District of California and elsewhere, the defendant,

ALEXEI VIKTOROVICH BILUCHENKO,

and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of a money transmitting business affecting interstate and foreign commerce, to wit, [redacted] "BTC-e" [redacted] and which:

a. failed to comply with the money transmitting business registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5) and 1022.380(a)(2); and

b. otherwise involved the transportation and transmission of funds known to the defendant to have been derived from a criminal offense and intended to be used to promote and support unlawful activity,

and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1960 & 2.

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

29. The factual allegations in paragraphs 1 through 26 are re-alleged and incorporated herein as if set forth in full.

30. From in or around 2011, continuing through a date unknown to the grand jury but no later

than in or around 2018, both dates being approximate and inclusive, within the Northern District of California, and elsewhere, the defendant,

ALEXEI VIKTOROVICH BILUCHENKO,

willfully and knowingly did combine, conspire, confederate, and agree together and with individuals known and unknown, to knowingly conduct and attempt to conduct financial transactions affecting interstate and foreign commerce which involved the proceeds of a specified unlawful activity, to wit:

a. operation of an unregistered money transmitting business, in violation of Title 18, United States Code, Section 1960

b. computer hacking and intrusions, in violation of Title 18, United States Code, Section 1030;

c. identity theft, in violation of Title 18, United States Code, Section 1028

d. interstate transportation of stolen property, in violation of Title 18, United States Code, Section 2314;

e. theft of government proceeds and extortion, in violation of Title 18, United States Code, Sections 641 and 1951; and

f. narcotics trafficking, in violation of Title 21, United States Code, Section 841,

with the intent to promote the carrying on of the specified unlawful activity, and knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transaction, knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

31. All of the allegations contained in this Indictment are re-alleged and by this reference fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Section 982(a)(1).

32. Upon a conviction for the offenses alleged in Counts 1 through 3 of this Indictment, the

defendant,

ALEXEI VIKTOROVICH BILUCHENKO,

shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal, involved in those offenses or any property traceable to such offenses

If any of the aforementioned property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

any and all interest the defendant has in other property, up to the value of the property described above, shall be vested in the United States and forfeited to the United States pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1).

All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal Rules of Criminal Procedure.

DATED: 7/12/2022

A TRUE BILL.

/s/
FOREPERSON

STEPHANIE M. HINDS
United States Attorney

*/s/ Claudia Quiroz*
CLAUDIA QUIROZ
Assistant United States Attorney

*/s/ C. Alden Pelker*
C. ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
United States Department of Justice